AMENDMENTS TO THE CLAIMS:

The listing of claims will replace all prior versions, and listings of claims in the application:

LISTING OF THE CLAIMS

1. (Currently amended) A method for transparent sign-on in a client-server environment, the method comprising the steps of:

receiving an encrypted communication on an originating server from a client, the client using a browser, the originating server belonging to at least one federation of trusted originating servers, each trusted originating server in the federation trusting the other originating servers in the federation;

creating a challenge string at the originating server;

sending an encrypted communication including the challenge string to a central sign-on server from the originating server;

recognizing the client by the central sign-on server;

receiving an encrypted communication on the originating server from the central sign-on server, wherein the communication received on the originating server includes a response to the communication sent to the central sign-on server and a first parameter based on the recognizing;

receiving client authenticating information from the client using the browser if the received first parameter indicates no session present for the client on any of the servers in the federation of trusted originating servers;

using client authenticating information provided in the response to the communication sent to the central sign-on server if the received first parameter indicates a session is present for the client on any of the servers in the federation of trusted originating servers;

~~updating~~ initiating a client session on the originating server; and sending another encrypted communication to the central sign-on server from the originating server.

2. (Original) The method of claim 1, wherein the step of creating a challenge

further comprises the step of recording on the originating server a URL requested by the client browser, a time at which the challenge was generated, and a federation identification.

3. (Original) The method of claim 2, wherein the step of sending an encrypted communication to a central sign-on server further comprises the steps of redirecting the client browser to the central sign-on server and sending to the central sign-on server the federation identification, the challenge, and a server identification.

4. (Original) The method of claim 1, wherein the step of receiving an encrypted communication on the originating server from the central sign-on server further comprises the step of receiving a digital signature of the central sign-on server for all information communicated from the central sign-on server.

5. (Original) The method of claim 4, wherein the step of receiving an encrypted communication on the originating server from the central sign-on server further comprises the step of receiving a redirection of the client browser on the originating server.

6. (Currently amended) The method of claim 5, wherein the step of receiving a redirection of the client browser further comprises the steps of receiving ~~a parameter indicating that no session was present on the central sign-on server,~~ the challenge, and the digital signature on all of the information communicated from the central sign-on server.

7. (Currently amended) The method of claim ~~5, wherein the step of receiving a redirection of the client browser further comprises the steps of receiving a parameter indicating that a session was present on the central sign-on server, the challenge, and the digital signature on all of the information communicated from the central sign-on server~~ 1, wherein the recognizing step comprises recognizing the client by the central sign-on server based on a cookie having a unique value previously stored on the client browser by the central sign-on server.

8. (Currently amended) The method of claim 1, ~~wherein~~ further including the step of ~~creating a client session on the originating server further comprises receiving~~

~~authenticating information from the client browser~~ redirecting the client browser to a requested URL based on a successful transparent sign-on.

9. (Canceled)

10. (Original) The method of claim 1, wherein the step of sending another encrypted communication to the central sign-on server from the originating server further comprises the step of creating a digital signature on all information sent to the central sign-on server.

11. (Currently amended) The method of claim 10, wherein the step of sending another encrypted communication to the central sign-on server further comprises the step of sending the challenge, a session time-out value, a second parameter specifying that a session has been ~~created~~ initiated on the originating server, a log-in identification of the client for which the session has been created, and the digital signature.

12. (Currently amended) A method for transparent sign-on in a client-server environment, the method comprising the steps of:

receiving an encrypted communication including a web-server-created challenge string on a central sign-on server, wherein the communication is from ~~a~~ the web server;

recognizing a client on the central sign-on server based on a previously initiated session on at least one of a federation of trusted servers, the web server comprising one of the trusted servers, each trusted server trusting the remaining trusted servers in the federation;

sending an encrypted communication to the web server from the central sign-on server including a first parameter based on the recognizing; and

receiving another encrypted communication including web-server-created session information on the central sign-on server from the web server.

13. (Currently amended) The method of claim 12, wherein the step of receiving an encrypted communication on the central sign-on server from the web server comprises the steps of receiving a redirection of the client browser on the

central sign-on server and receiving a federation identification, ~~a~~ the challenge, an identification of the web server, and a digital signature of the web server.

14. (Original) The method of claim 12, wherein the step of recognizing the client on the central sign-on server further comprises the steps of creating a cookie on the client browser and creating a record of the client on the central sign-on server.

15. (Original) The method of claim 14, wherein the step of creating a record of the client on the central sign-on server further comprises the step of using the cookie and the identification of the originating server as a concatenated primary key.

16. (Original) The method of claim 12, wherein the step of recognizing the client on the central sign-on server comprises the steps of accessing a cookie on the client browser and looking up the client on the central sign-in server based on the cookie.

17. (Original) The method of claim 16, wherein the step of looking up the client based on the cookie comprises looking up the challenge associated with the client session from a record on the central sign-on server.

18. (Original) The method of claim 12, wherein the step of sending an encrypted communication to the web server from the central sign-on server comprises the step of creating a digital signature for all information communicated to the web server.

19. (Original) The method of claim 18, wherein the step of sending an encrypted communication to the web server from the central sign-on server further comprises the steps of redirecting the client browser back to the web server and communicating the client log-in identification for the current client session, the challenge, and the digital signature.

20. (Currently amended) The method of claim 18, wherein the step of sending an encrypted communication to the web server from the central sign-on server further comprises the steps of redirecting the client browser back to the web server

and communicating ~~a~~ the first parameter indicating that no session was present on the central sign-on server, the challenge, and the digital signature.

21. (Currently amended) The method of claim 12, wherein the step of receiving another encrypted communication on the central sign-on server further comprises the steps of receiving an identification of the web server, ~~a~~ the challenge, a session time-out value, and a digital signature for all information sent to the central sign-on server.

22. (Currently amended) The method of claim 21, wherein the step of receiving another encrypted communication on the central sign-on server further comprises receiving a second parameter specifying that a session has been created on the web server and a log-in identification of the client for which the session has been created.

23. (Original) The method of claim 12, further comprising the step of updating a record of the client session on the central sign-on server.

24. (Original) The method of claim 23, wherein the step of updating a record of the client session on the central sign-on server comprises the step of verifying a digital signature of the web server.

25. (Original) The method of claim 24, wherein the step of updating a record of the client session on a central sign-on server further comprises the steps of creating a record on the central sign-on server of the client session and the session time-out value.

26. (Currently amended) A method for session maintenance in a transparent sign-on client-server environment, the method comprising the steps of:

running a session freshening task for sessions on ~~a~~ each web server of a plurality of web servers, each web server comprising a trusted server included in a federation of trusted servers, each trusted server trusting the remaining trusted servers in the federation;

sending an encrypted communication including a web-server-created

challenge string to a central sign-on server from ~~the~~ each web server; and

recognizing ~~a~~ an associated session on the central sign-on server.

27. (Original) The method of claim 26, wherein the step of running a session freshening task comprises the steps of looking up a list of active sessions on the web server and determining whether a session will expire on the central sign-on server before the next time the session freshening task runs.

28. (Original) The method of claim 27, wherein the step of sending an encrypted communication to the central sign-on server from the web server comprises the step of sending a server identification of the web server, the challenge used in creating the session, a new time-out value for the session, and a digital signature for all information sent in the message.

29. (Original) The method of claim 28, wherein the step of recognizing a session on the central sign-on server comprises the steps of verifying the digital signature and using the challenge to look up a record of the sessions on the central sign-on server.

30. (Original) The method of claim 26, further comprising the step of updating a client session record associated with the session on the central sign-on server.

31. (Original) The method of claim 30, wherein the step of updating a client session record comprises the step of updating a time-out value for the session on the central sign-on server.

32. (Currently amended) A method for session maintenance in a transparent sign-on client server environment, the method comprising the steps of:

recognizing a client on a web server, the web server belonging to at least one federation of trusted web servers, each trusted web server trusting the remaining web servers in the federation;

terminating a client session on the web server;

sending an encrypted message including a web-server-created challenge string to a central sign-on server;

recognizing the client on the central sign-on server;

updating a record of a session associated with the client;

sending an encrypted communication from the central sign-on server to a second trusted web server, the second trusted web server having a current local session associated with the client; and

terminating ~~a~~ the local session associated with the client at the second trusted web server.

33. (Currently amended) The method of claim 32, wherein the step of recognizing the client on the web server comprises the step of looking up ~~a~~ the web-server-created challenge associated with a client session.

34. (Original) The method of claim 33, wherein the step of recognizing the client on the web server comprises receiving a communication from the client.

35. (Original) The method of claim 33, wherein a digital signature is created for all information communicated to the central sign-on server.

36. (Original) The method of claim 35, wherein the step of recognizing the client on the central sign-on server comprises the steps of verifying the digital signature of the web server and using the challenge to look up a record of any current session associated with the client.

37. (Original) The method of claim 32, wherein the step of updating a record of a session associated with the client comprises deleting a record on the central sign-on server.

38. (Currently amended) The method for claim 32, wherein the step of sending an encrypted message to a second trusted web server further comprises sending the encrypted message to each web server for which the central sign-on server has a record of an active session associated with the client.

39. (Currently amended) The method of claim 38, wherein the step of sending an encrypted message to a second trusted web server further comprises the step of

sending a parameter indicating that the client session is terminated and a digital signature of the central sign-on server.

40. (Currently amended) The method of claim 39, wherein the step of terminating a local session associated with the client at the second trusted web further comprises the step of verifying the digital signature of the central sign-on server.

41. (Currently amended) A system for secure single sign-on in a client-server environment, the system comprising:

a ~~server~~ plurality of servers, ~~the~~ each server configured to communicate with ~~a~~ at least one client, each server being a member of at least one federation of trusted servers, each trusted server trusting the remaining servers in the federation;

a central sign-on server, the central sign-on server configured to communicate with the at least one client and ~~the~~ each server and to receive a server-created challenge string from the communicating server; and

means for identifying the at least one client on the central sign-on server.

42. (Currently amended) The system of claim 41, wherein the means for identifying the client on the central sign-on server comprises application code and script residing at a Single Sign-On Support URL located on ~~the~~ each server and known by the central sign-on server.

43. (Currently amended) The system of claim 42, wherein the Single Sign-On Support URL comprises means for creating ~~a~~ the challenge when the client initiates communication with the server, means for redirecting the client browser to the central sign-on server, means for communicating the challenge to the central sign-on server, and means for receiving a communication from the central sign-on server.

44. (Original) The system of claim 41, wherein the server and the central sign-on server are co-located on the same server.

45. (Currently amended) The system of claim 41, wherein ~~the server is a member of a federation of servers, where~~ each member of the federation of trusted servers is configured with a server identification, and configured to use a similar policy with regard to session management as a second server in the federation of trusted servers.

46. (Currently amended) The system of claim 45, wherein ~~the~~ each server in the federation of trusted servers is configured to send encrypted messages to the central sign-on server and receive encrypted messages from the central sign-on server.

47. (Currently amended) The system of claim 46, wherein the central sign-on server is a central sign-on server for more than one federation of trusted servers, each federation of trusted servers being configured with a unique federation identification.

48. (Currently amended) The system of claim 47, wherein the central sign-on server is configured to create a digital signature that is recognized by the server in the federation of trusted servers.